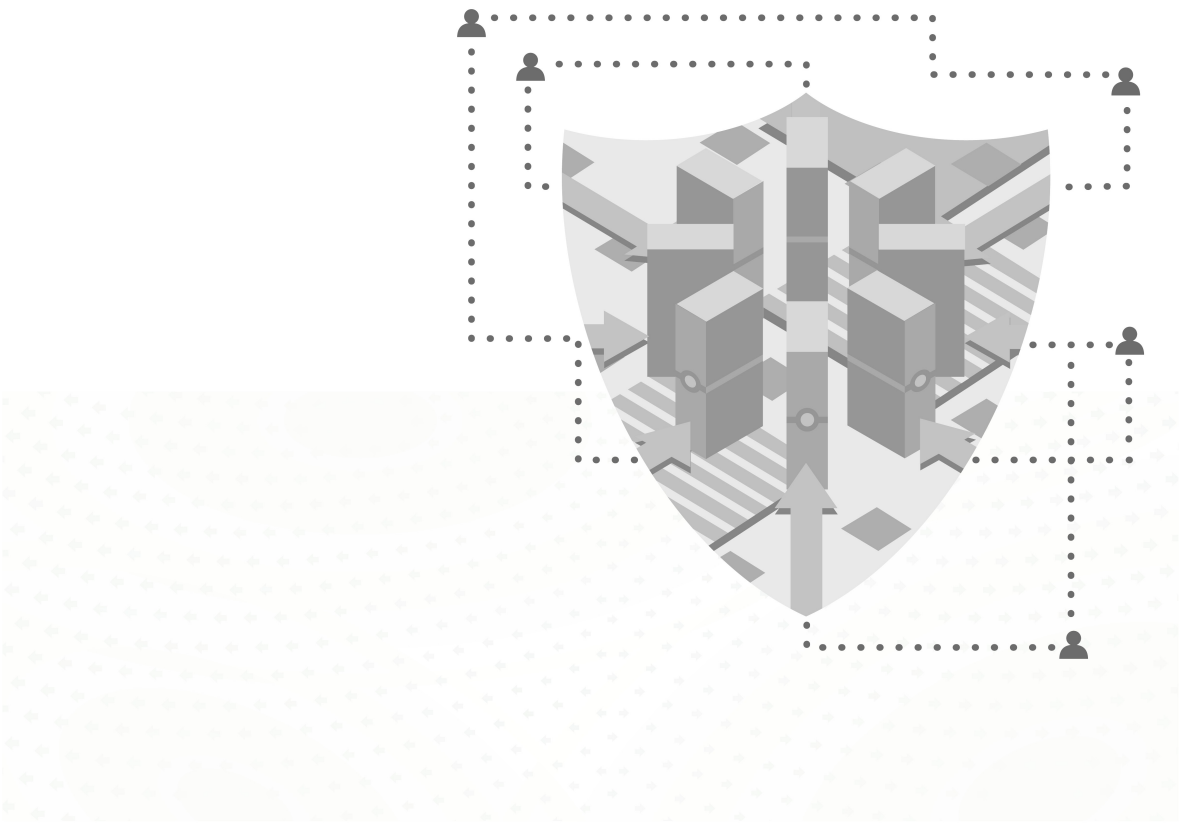
Sourcefire
SSL Appliance 2000/8200
Getting Started Guide

Software v. 3.7.1
Document Revision 04/02/2014



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

Legal Notices

Cisco, the Cisco logo, Sourcefire, the Sourcefire logo, Snort, the Snort and Pig logo, and certain other trademarks and logos are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Cisco or its subsidiaries (collectively, "Cisco") or any Sourcefire-provided or Cisco-provided products. Sourcefire and Cisco products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

The copyright in the Documentation is owned by Cisco and is protected by copyright and other intellectual property laws of the United States and other countries. You may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Cisco's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

No part of the Documentation may be used in a compilation or otherwise incorporated into another work or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of Cisco. Cisco reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms.

© 2004 - 2014 Cisco and/or its affiliates. All rights reserved.

Disclaimers

THE DOCUMENTATION AND ANY INFORMATION AVAILABLE FROM IT MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. CISCO MAY CHANGE THE DOCUMENTATION FROM TIME TO TIME. CISCO MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE ACCURACY OR SUITABILITY OF ANY CISCO-CONTROLLED WEBSITE, THE DOCUMENTATION AND/OR ANY PRODUCT INFORMATION. CISCO-CONTROLLED WEBSITES, THE DOCUMENTATION AND ALL PRODUCT INFORMATION ARE PROVIDED "AS IS" AND CISCO DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL CISCO BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF PROFITS, AND/OR BUSINESS INTERRUPTIONS), ARISING OUT OF OR IN ANY WAY RELATED TO CISCO-CONTROLLED WEBSITES OR THE DOCUMENTATION, NO MATTER HOW CAUSED AND/OR WHETHER BASED ON CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER TORTUOUS ACTIVITY, OR ANY OTHER THEORY OF LIABILITY, EVEN IF CISCO IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Contents

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

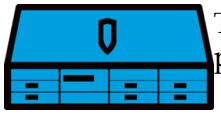
1. Introduction

The following conventions are used throughout this document.

This symbol indicates a "note" providing additional information that the reader may be interested in.

! This symbol indicates a "warning" providing additional information that the reader needs to pay attention to.


This symbol indicates information that only applies to the Sourcefire SSL Appliance 2000, also called the SSL2000.


This symbol indicates information that only applies to the Sourcefire SSL Appliance 8200, also called the SSL8200.

Throughout this document the term SSL is used to mean both SSL and TLS, unless explicitly indicated. Secure Socket Layer (SSL) has been largely replaced by Transport Layer Security (TLS) which is the more up to date standard derived from SSL. Both SSL and TLS traffic are present in networks today and the Sourcefire SSL appliance is capable of inspecting both types of traffic.

! The embedded software contained within the Sourcefire SSL appliance is subject to licensing terms and conditions imposed by Sourcefire and third party software providers. You should only use the Sourcefire SSL appliance if you agree to these licensing conditions; see the *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* for licensing details.

! The act of "inspecting" SSL traffic may be subject to corporate policy guidelines and/or national legislation. It is your responsibility to ensure that your use of the Sourcefire SSL appliance is in accordance with any such legal or policy requirements.

This guide describes how to get started using the Sourcefire SSL appliance. It shows how to configure the minimum set of system options and provides basic examples showing how to configure the device to operate in two common modes. The *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* provides full details on all of the options available in the SSL2000 and SSL8200 and should be consulted for more complex configurations.

1.1 Components

Carefully unpack the Sourcefire SSL appliance and compare the actual contents with Table 1 to ensure that you have received all ordered components. Follow the instructions in Section 2. to install and set up the appliance.

Part	Description	Quantity
Sourcefire SSL2000 or SSL8200 appliance	1U or 2U rack mountable device	1
2 x Power Cords	One for each redundant supply	2
Rack mounting rails	Rails to rack mount the device	1
	Number of Components	**4**

Table 1: SSL2000/SSL8200 Packing List

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

2. Physical Installation

This section describes the following procedures:

- Installing the Sourcefire SSL appliance as a rack-mounted component; and
- Connecting the Sourcefire SSL appliance to the network.

2.1 Safety Information

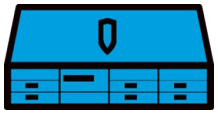
Because this is an electrically powered device, adhere to the warnings and cautions listed in this document when installing or working with the Sourcefire SSL appliance.

WARNING: Read all the installation instructions before connecting the appliance to its power source. Refer to the *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* for more information regarding the setup and placement of the Sourcefire SSL appliance.

2.2 Requirements Checklist

The following will be required:

- At least 1U rack space (deep enough for a 27" device); power and management ports at rear
- Phillips (cross-head) screwdriver
- Two available power outlets (110 VAC or 220-240 VAC)
- Two IEC-320 power cords (normal server/PC power cords) should the supplied power cords not be suitable for your environment
- Cooling for an appliance with two 650W power supply units
- One RJ-45 CAT5e/CAT6 Ethernet cable to connect the Sourcefire SSL appliance to the management network (or a local notebook/desktop computer which is used to manage the Sourcefire SSL appliance)
- Appropriate copper or fiber cables to connect Netmods to the network and to associated security appliances



The following will be required:

- At least 2U rack space (deep enough for a 27" device); power and management ports at rear
- Phillips (cross-head) screwdriver
- Two available power outlets (110 VAC or 220-240 VAC)
- Two IEC-320 power cords (normal server/PC power cords) should the supplied power cords not be suitable for your environment
- Cooling for an appliance with two 750W power supply units

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

- One RJ-45 CAT5e/CAT6 Ethernet cable to connect the Sourcefire SSL appliance to the management network (or a local notebook/desktop computer which is used to manage the Sourcefire SSL appliance)
- Appropriate copper or fiber cables to connect Netmods to the network and to associated security appliances

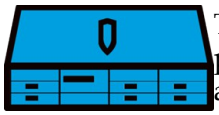
2.3 Rack Mounting

The Sourcefire SSL appliance is equipped with pre-installed rack-mount brackets and supplied with rack mount rails allowing easy installation in a rack.

2.4 Back Panel

The rear of the SSL2000 is shown in Figure 2.1 and Table 2 identifies the components. Ventilation holes on the rear panel must not be blocked as free flow of air is essential for system cooling.

Figure 2.1: SSL2000 Back Panel



The rear of the SSL8200 is shown in Figure 2.2 and Table 2 identifies the components. Ventilation holes on the rear panel must not be blocked as free flow of air is essential for system cooling.

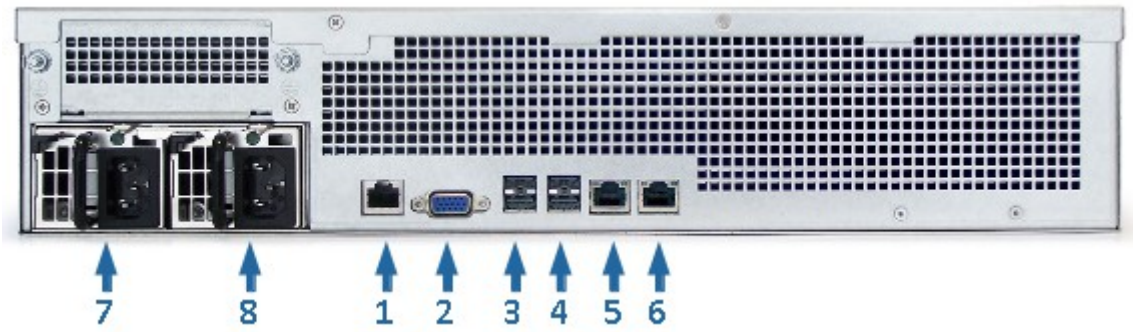


Figure 2.2: SSL8200 Back Panel

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

1	Serial Port	5	Management Ethernet 1
2	VGA Display Connector	6	Management Ethernet 2
3	USB Port	7	Power Supply 1
4	USB Port	8	Power Supply 2
		*	7, 8 not shown in Figure 2.1

Table 2: SSL2000 & SSL8200 Back Panel Components

The Sourcefire SSL appliance is equipped with two independent power supply units, either of which can power the appliance. The power supply units feature IEC-320 (that is, standard server/PC style) connectors. Normally both units should be attached to an uninterruptible power supply or other power outlet (110 or 220/240 Volt AC).

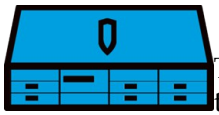
The power supplies are hot swappable and can be replaced while the Sourcefire SSL appliance is powered on and operating.

Replacement must be done with units supplied by Sourcefire. Use of other units will void any warranty and may damage the system.

2.5 Front Panel

The SSL2000 has three front-facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Up to 12 GigE or up to 6 10 GigE interfaces can be installed. Figure 2.3 shows the front panel of an SSL2000 that has 12 GigE copper interfaces.

Figure 2.3: SSL2000 Front Panel



The SSL8200 has 7 front-facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the seven bays to configure the desired combination of interfaces.

Sourcefire recommends restricting an SSL8200 to supporting a maximum of 16 external interfaces. This means that if 4 x GigE Netmods are used a maximum of four can be installed in the system.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 2.4: SSL8200 Front Panel

Figure 2.4 shows an SSL8200 device with four Netmods installed. In this example two of the Netmods each support 4 x GigE fiber interfaces and the other two 4 x GigE copper interfaces.

The following Netmod types can be used in an SSL2000:

- 4 x GigE copper (4 ports of 10/100/1000Base-T with bypass)
- 4 x GigE fiber (4 ports of 10/100/1000Base-SX with bypass)
- 2×10Gig fiber (2 ports of 10GBase-SR with bypass)
- 2×10Gig fiber (2 ports of 10GBase-LR with bypass)

! Netmods are NOT hot swappable, and should only be swapped when the system is powered off. See the *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* for details.

The front panel has indicators, buttons an LCD display and a USB port that the administrator can use to configure and diagnose the system. The relevant portion of the front panel is shown in Figure 2.5. Table 3 identifies the components.

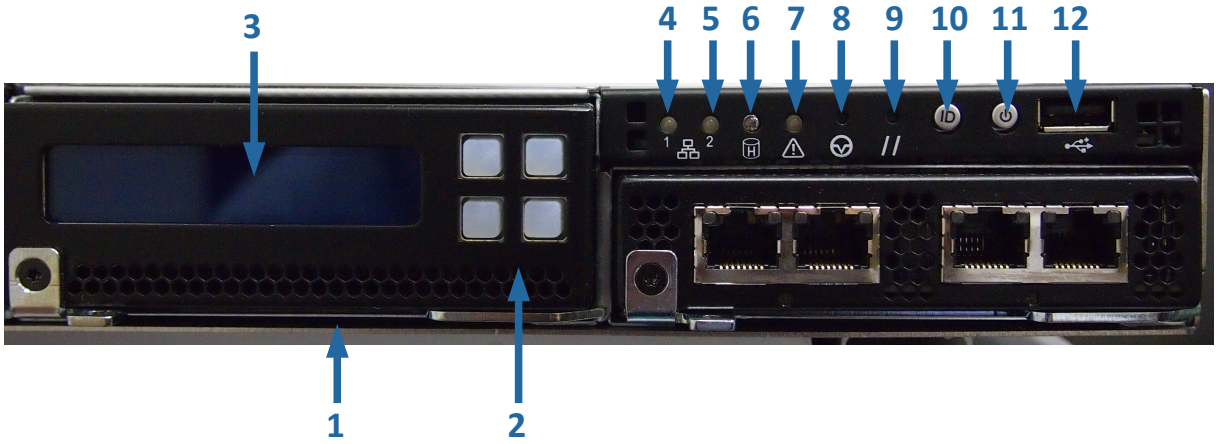


Figure 2.5: SSL2000 Front Panel Controls

Figure 2.6 shows the front panel controls on an SSL8200 and Table 3 identifies the components.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

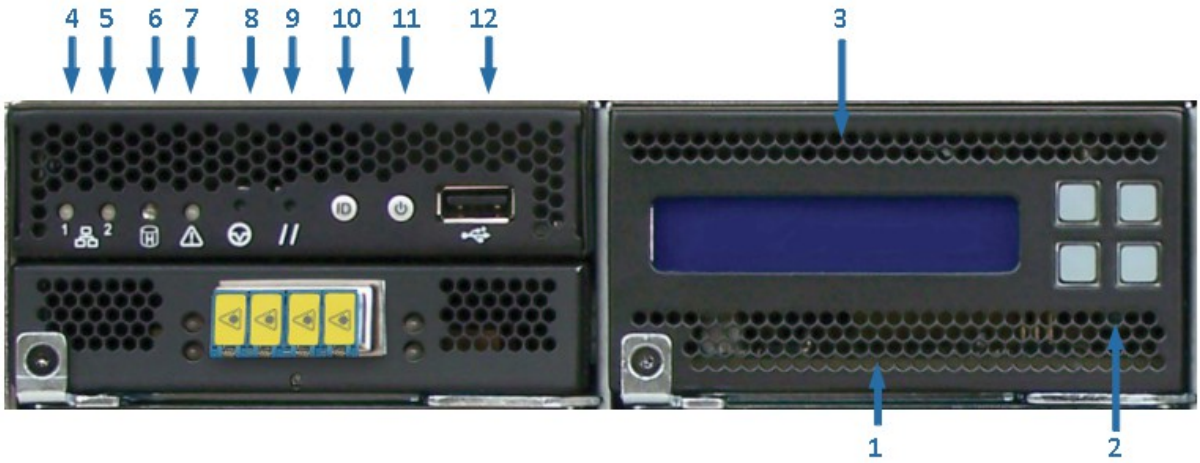


Figure 2.6: SSL8200 Front Panel Controls

1	Switch Module	7	System Status Indicator
2	Keypad Array	8	NMI button (recessed)
3	LCD Display	9	Reset button (recessed)
4	Management Ethernet 1 Indicator	10	Identify Button
5	Management Ethernet 2 Indicator	11	Power Button
6	Disk Activity Indicator	12	USB socket

Table 3: SSL2000 & SSL8200 Front Panel Components

The front panel LEDs for the rear panel Management Ethernet ports are green when the link is up, and flash amber/yellow to indicate traffic flowing over the link. The two LEDs that are part of each Ethernet port on the rear panel indicate the operating speed of the link and if data is flowing over the link. The left LED viewed from the back of the unit is green if the link is up and flashes to indicate traffic flow. The right LED can be: off (10 Mbps connection), green (a 100 Mbps connection) or amber (a GigE connection).

The disk activity LED is green and flashes when there is any disk activity on a SATA port in the system.

The system status LED is green/amber, and the various display options indicated different system states.

Table 4 shows the various system states that can be indicated by the system status LED on the front panel of the unit.

The NMI and Reset buttons are recessed, requiring the use of a straight thin object to press the button. Pressing the Reset button will cause the system to be reset. The NMI button should not be pressed during normal operation as it may cause the system to halt. If the NMI button is pressed this fact will be recorded in the system log file.

The ID button if pressed will cause a blue LED on the rear panel to the left of the serial port to illuminate. The purpose of this LED is to make it easier to locate a system when it is racked in a stack with other systems.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Color	State	System status	Meaning
Green	Solid	OK	System ready – no errors detected
Green	Blink	Degraded	Memory, fan, power supply or PCIe failures
Amber	Solid	Fatal	Alarm – system has failed and shut down
Amber	Blink	Non-Fatal	Alarm – system likely to fail – voltage/temp warnings
Green + Amber	Solid	OK	First 30 seconds after AC power connected
None	Off	Power off	AC or DC power is off

Table 4: SSL2000 & SSL8200 System Status Indicators

2.6 Connecting the Management Network

The WebUI management interface is accessed via Management Ethernet 1. Plug a cable into the Ethernet port identified as Management Ethernet 1 in Figure 2.1 or Figure 2.2. Check that the LEDs on the port indicate that the link is up.

2.7 Connecting to the Network and Attached Appliance

The SSL2000 and SSL8200 products have front-facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the bays to configure the desired combination of interfaces. Figure 2.3 shows an SSL2000 device with three Netmods installed. In this example the Netmods each support 4×10/100/100 copper interfaces. Available Netmod options are listed below; other Netmod types may become available in the future:

- 4 x GigE copper (4 ports of 10/100/1000Base-T with bypass)
- 4 x GigE fiber (4 ports of 10/100/1000Base-SX with bypass)
- 2 x10Gig fiber (2 ports of 10GBase-SR with bypass)
- 2 x10Gig fiber (2 ports of 10GBase-LR with bypass)

! **Netmods are NOT hot swappable and should only be swapped when the system is powered off.** See the *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* for details.

Ports are numbered from left to right and top to bottom in the case of the SSL8200 when facing the front of the device. When a segment is configured and activated the port numbers allocated to that segment are displayed on the management WebUI. The relevant ports will need to be connected to the network and associated security appliance(s) using appropriate copper or fiber cabling.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

3. Power On and Initial Configuration

Ensure that the two power supplies are connected to power using appropriate cabling. To turn the unit on press the front panel power button, which is shown in Figure 2.5. If all is well the System Status Indicator will be solid green, and after a minute or so the LCD display will illuminate and display a message similar to that in Figure 3.1.

Figure 3.1: Initial LCD Display after Power On

The initial screen shown in Figure 3.1 will appear for a while and then the LCD will blank before displaying the message shown in Figure 3.2.

Figure 3.2: Power on Message: Detecting HD

Figure 3.3: Power on Message: Loading Failsafe Indication

After the system has detected the SSD (Figure 3.2) and the Disk on Module (Figure 3.3) it will boot from the SSD and display the message shown in Figure 3.4.

Figure 3.4: Power on Message: Booting HD

Once the system has booted, the display changes to indicate that the keypad is now active and can be used to access menu options. Figure 3.8 shows the display with an arrow at the bottom right of the display, indicating that the bottom right button on the keypad is active. The two symbols at the right of the display correspond to the two rightmost buttons on the keypad; if all four buttons of the keypad are active, four symbols are displayed.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 3.5: Power on Display: Booting File System

Figure 3.6: Booting

Figure 3.7: Power on Display: Validating Firmware

Figure 3.8: Power on Display: Boot Complete

Pressing the bottom right button repeatedly will show the Network screen. Pressing the top left button will enter the Network submenu and display the IP address of the system. Figure 3.9 shows the Network option. Figure 3.10 shows the IP address display.

Figure 3.9: Network Menu

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 3.10: IP Address

Figure 3.11: Mask Address

Figure 3.12: Gateway Address

The final screen is blank. After that, the appliance shows the boot complete screen again (as in Figure 3.8).

Take a note of the IP address, as this will be needed to access the WebUI in order to continue setting up the device. Refer to the *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* for details of how to configure an IP address if the management network is not using DHCP.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

4. System Bootstrap Phase

If the basic system information has not been configured, the device will enter the "bootstrap" phase when powered on. To enter the minimum necessary information required by the system before it will exit the bootstrap mode, a connection is required to the WebUI. Using a web browser open a session to the IP address that is being used by the SSL2000 and SSL8200. For the example address of 192.168.2.42, accessing the following URL will connect to the WebUI.

```
https://192.168.2.42
```

The first step is shown in Figure 4.1, and only occurs if the master key mode is not already configured. Configure where the Master Key for the SSL2000 and SSL8200 is stored, and whether or not it is password protected. In this example the default options are used, so no password is required and the master key is stored internally. Simply click on the Next button, shown in Figure 4.1, to continue configuring the device.

Figure 4.1: Bootstrap Master Key Mode

The final stage of the bootstrap process is user setup (Figure 4.2). At least one user with the Manage Appliance role and at least one with the Manage PKI role must be created; it can be one user with both roles, or two users. As soon as the users are created the system will exit bootstrap mode.

If the system has previously been configured and already has at least one user with the Manage Appliance role, and one with the Manage PKI role, this step will be skipped.

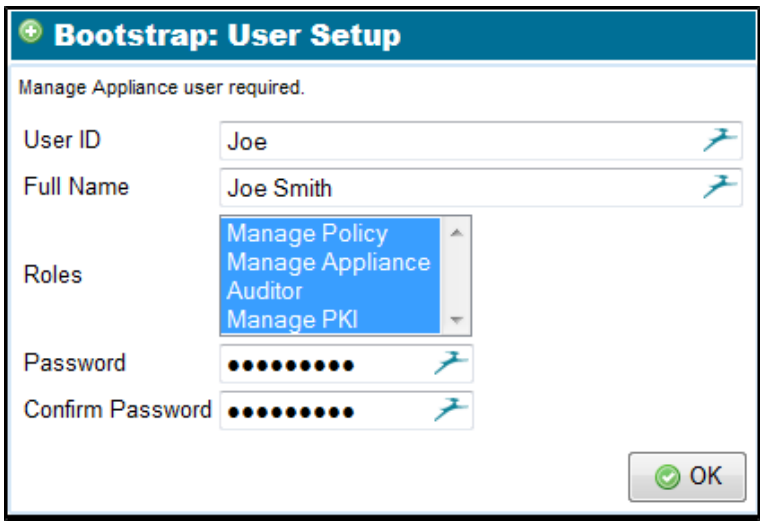


Figure 4.2: Bootstrap User Setup

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

5. Completing System Configuration

The following common steps are done once the system is out of the bootstrap phase.

An HTTPS connection to the IP address assigned to the Sourcefire SSL appliance management interface will produce the standard login window (Figure 5.1). Log on using the username and password created in Section 4..

Figure 5.1: Initial Access Login

The Sourcefire SSL appliance uses a self-signed SSL server certificate which may result in a warning message from the browser when connecting to the WebUI. The warning can be prevented by adding this self-signed certificate to your browser as a trusted device. Consult your browser documentation for details on how to add the Sourcefire SSL appliance as a trusted device.

5.1 Configuring Date and Time

To configure the system date and time use the **Date/Time** option on the device menu. Initially this menu will be labeled "localhost.localdomain". If you click on the Edit pencil icon, , at the top right of the **Date/Time** window (Figure 5.3) you can edit these settings. Figure 5.2 shows the edit screen.

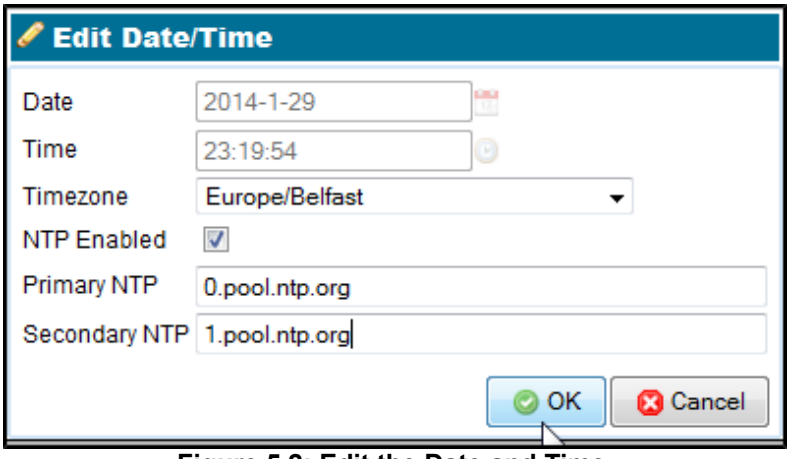


Figure 5.2: Edit the Date and Time

If **NTP** is enabled, as in this example, then the **Date** and **Time** fields will be disabled as these values are being set by the Network Time Protocol (**NTP**). In order for NTP to operate you need to configure a primary NTP server and ideally, a secondary NTP server. Once the settings are configured and the OK button is pressed to save the settings the screen will look like Figure 5.3.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Click the Reboot button to ensure that the time changes take effect; this will reboot the system.

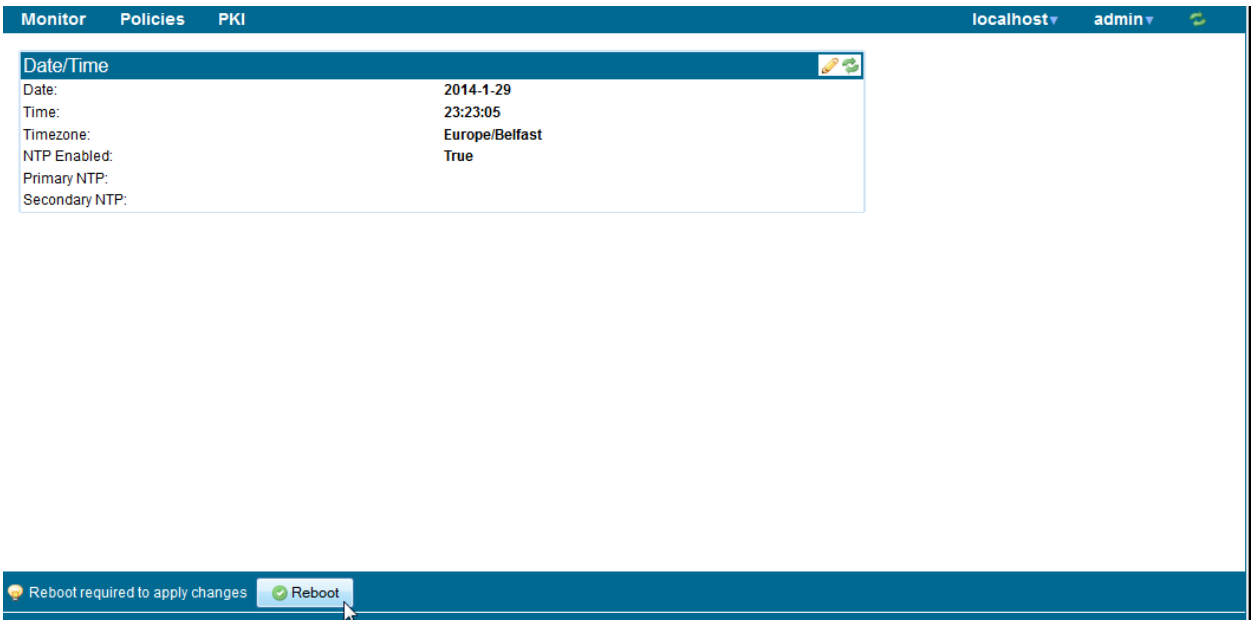


Figure 5.3: Time Settings with Reboot Button

On initial start up, the License status icon will be red, and you will see a warning message. See the *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* for details on setting up users, implementing any license(s), and other post initial setup details.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

6. Configuring PKI

The two example inspection configurations provided later in the document make use of a known server key and certificate that needs to be loaded into the SSL2000 or SSL8200 and use certificate resign which requires that the SSL2000 and SSL8200 has a CA certificate. This section details how to set up these certificates on the system. It is assumed that a local SSL server is available, and that a copy of the private key and SSL server certificate are available.

6.1 Installing a CA for Certificate Resign

Before the Sourcefire SSL appliance can be used to inspect traffic using Certificate Resign mechanisms it must have at least one CA certificate and private key installed to do the resigning. A CA can either be created by the Sourcefire SSL appliance and self-signed or sent off for signing by another CA), or it can be imported. Management of Internal Certificate Authorities is done using the menu option on the **PKI** menu.

Figure 6.1 shows the screen when there are no Internal Certificate Authorities in the system. The icons at the top right allow the user to:

- Generate a new Internal Certificate Authority: 
- Add an Internal Certificate Authority by importing an existing CA and key: 

Figure 6.1: Empty Internal Certificate Authority Window

The simplest approach is to generate an internal self-signed CA certificate. Clicking on the icon to generate a CA will produce the **Generate Certificate** window shown in Figure 6.2. This allows the basic data required in a CA to be input and the key size and validity period to be specified. Input the data and then click the Generate self-signed CA button.

Figure 6.2: Generate Internal Certificate Authority Field

As this CA is self-signed, it will not be trusted by a client system until it has been exported and added to the list of trusted CAs on the client system. When the OK button is clicked, the certificate is saved and installed. An entry in the Internal Certificate Authorities table appears with an indication that no CSR has been generated for this certificate.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

To download the CA certificate so you can install it on the client system, click to select the entry, then click on the export certificate button. Consult your browser documentation for details on how to add this CA to the browser's list of trusted CAs.

6.2 Importing Known Server Keys

To inspect traffic to an internal SSL server, the easiest approach is to use known server key and certificate mode which requires that a copy of the server's SSL certificate and private key are loaded into the SSL2000 or SSL8200. Known server certificates and keys are imported into the all-known-certificates-with-keys list. The **Known Certificates and Keys** option on the **PKI** menu is used to import new certificates and keys.

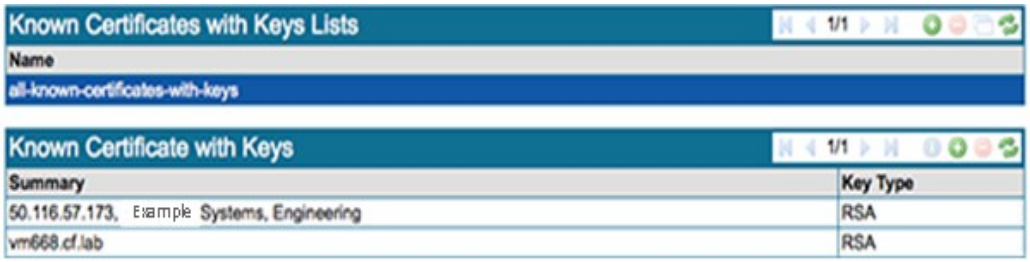


Figure 6.3: Known Certificate with Keys Display

There are two windows, one for choosing the list that is to be operated on, and the other to manipulate the contents of that list. In this example the key/certificate will be added to the **all-known-certificates-with-keys** list. Figure 6.3 shows the initial appearance of the input forms.

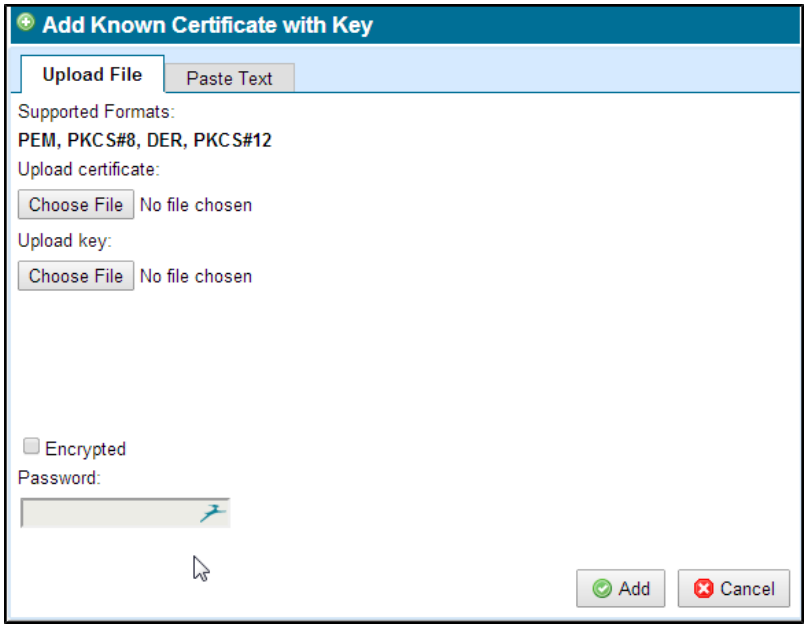


Figure 6.4: Import Known Certificate with Keys

Click to select the **all-known-certificates-with-keys** list and then click on the Add button, . Figure 6.4 shows the input form that will appear. You can then either specify the file to import or paste in the key and certificate details, and then click the Add button. If the key and certificate are valid then a message confirming that the Certificate has been added will appear with a button that allows you to view the details of the imported certificate. You will also see that the key now appears as a row in the **Known Certificate with Keys** window.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 6.5 shows the screen after a number of keys have been imported and shows the Apply button that needs to be used to save the imported certificates and keys to the secure store.

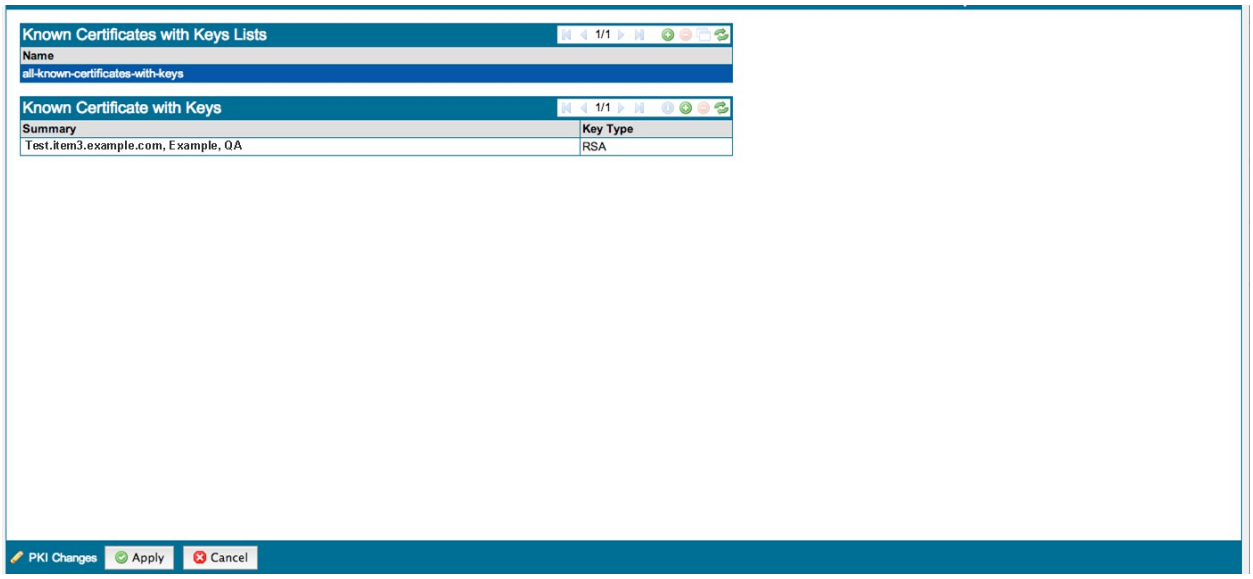


Figure 6.5: Known Certificate and Keys

Load the key/certificate for each local SSL server that you wish to inspect traffic to.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

7. Example Passive-Tap Mode Inspection

The following example shows the steps to configure the Sourcefire SSL appliance to inspect traffic using the known key/certificate mode, with the SSL2000 and SSL8200 connected in passive-tap mode. The simplest passive-tap configuration is one port on the SSL2000 and SSL8200, which receives a copy of network traffic from a network tap device, and one port on the SSL2000 and SSL8200 that sends traffic to the attached security appliance.

The steps involved are:

- Load the server key/certificate into the Sourcefire SSL appliance (see section 6.2)
- Create a ruleset that contains a rule to inspect traffic to the server
- Create a segment for passive-tap operation
- Activate the segment to start inspection

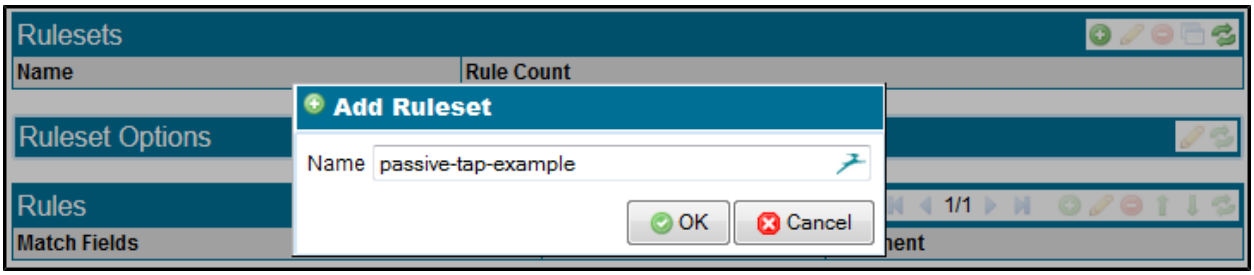


Figure 7.1: Adding a Ruleset

Creating a ruleset is a two-step process: first create the ruleset to hold the rule and then define the rule itself. Figure 7.1 shows the screen while adding a new ruleset called passive-tap-example; the **Add Ruleset** box is accessed by clicking on the button in the **Rulesets** panel toolbar. After giving the ruleset a name click OK. The new entry will appear as a row in the **Rulesets** grid and is available for use. At the bottom of the screen is a **Policy Change**s area with buttons to Apply or Cancel the change. Click Apply to complete the process and to save the ruleset to disk.

Now click on the "passive-tap-example" row to select it. This will cause the **Ruleset Options** for this ruleset to be displayed. In this example the default settings are fine.

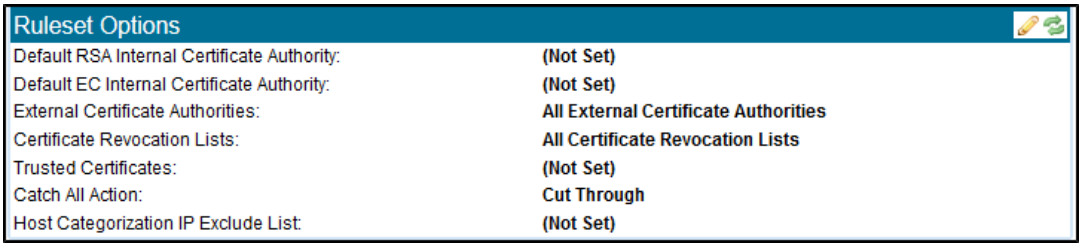


Figure 7.2: Ruleset Options

The **Rules** panel will also appear when the ruleset row is selected; clicking will cause the **Insert Rule** form (Figure 7.3) to appear, and selecting **Decrypt (Certificate and Key known)** on the drop-down menu in this form will let you configure the rule.

In this example the rule only applies to a single server for which the certificate and key are known, so the **Known Certificate with Key** option is checked and the system for which we loaded the key is selected from the drop-down menu. Apart from adding a comment to the **Comment** box, no other options are used in this rule so the Save button can be pressed to create the rule.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

At the bottom of the window, click Apply in the **Policy Changes** area to complete the process and save the rule to disk.

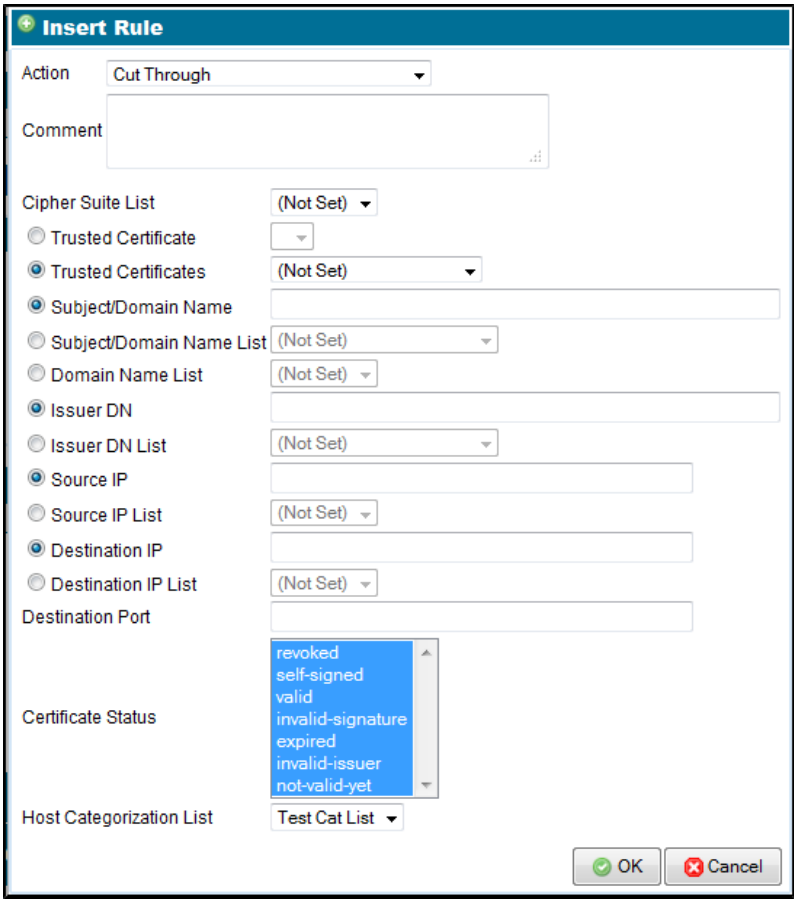


Figure 7.3: Add Encrypt using Known Server Key/Certificate Rule

The final part of the process is to create a segment, configure it to use the ruleset just created, and then to activate it. To create a **Segment** go to the **Policies > Segments** menu option and you will see the **Segments** panel. Figure 7.4 shows the segment screen when no segments currently exist on the system. In this example, the device is an SSL2000, as can be seen from the graphic at the top of the screen. The ports that show green on the graphic indicate that the links on these ports are up.

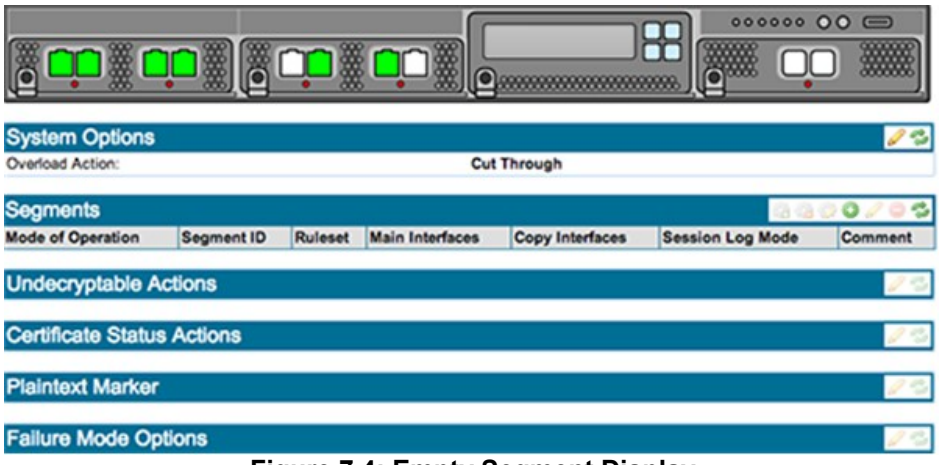


Figure 7.4: Empty Segment Display

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Initially there will be no segments configured in the system. To create a new segment, click the Add, , button in the **Segments** panel. Figure 7.5 shows the initial form. The **Mode of Operation** is selected by clicking on the Edit button, and then choosing from the **Select Mode of Operation** form the required mode. Select the **Ruleset** from the drop-down menu.

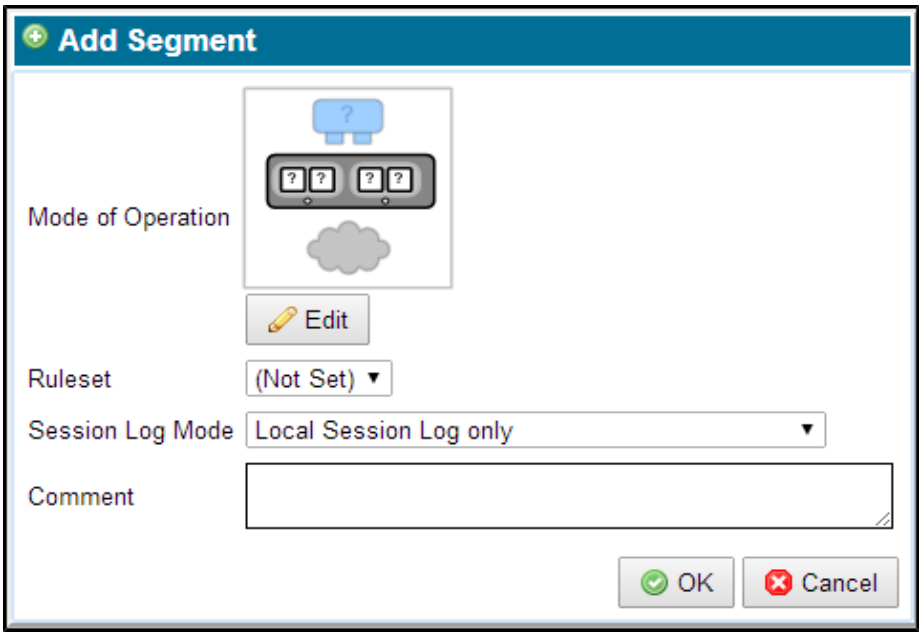


Figure 7.5: Add Segment

Figure 7.6 shows the **Add Segment** window used to select the mode of operation for a segment. The **Mode of Operation** area has an Edit button; click it to display the different operating modes as images, and select from them.

The **Main Mode** drop-down menu allows the set of operating modes to be narrowed by choosing only Passive Tap; this will reduce the number of options displayed in the **Mode of Operations** area. The **Asymmetric Sub-Mode** drop-down can be used to further narrow the number of modes of operation that are displayed. Clicking on the image for the desired operating mode selects it and clicking Save will set this as the mode of operation for the segment.

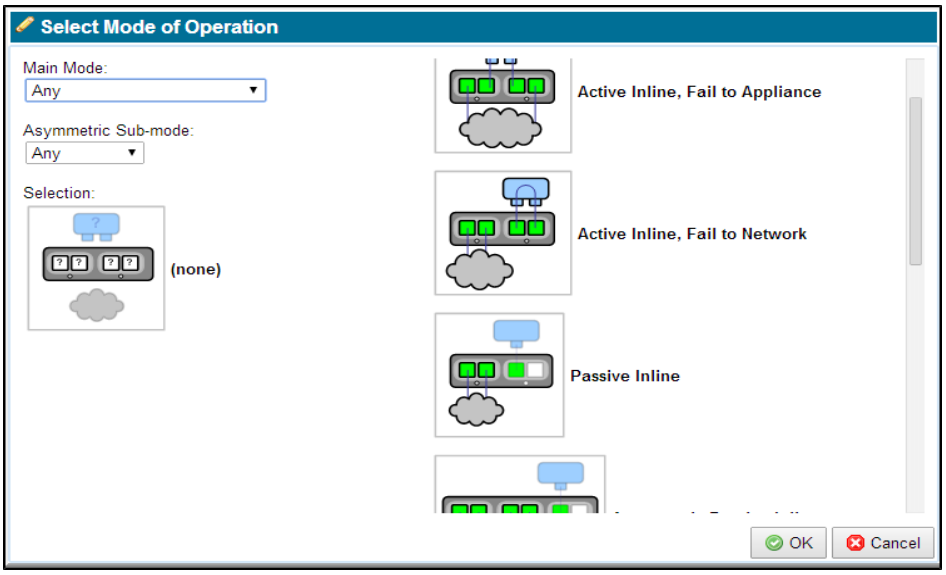


Figure 7.6: Selecting Mode of Operation for a Segment

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 7.7 shows the completed segment details before they are saved. In this example the session log has been enabled and the segment is using the "passive-tap-example" ruleset that was created earlier. The graphic in the field indicates that this segment will make use of two ports on the system, the actual port numbers to be used are not known at this point, they are determined when the segment is activated.

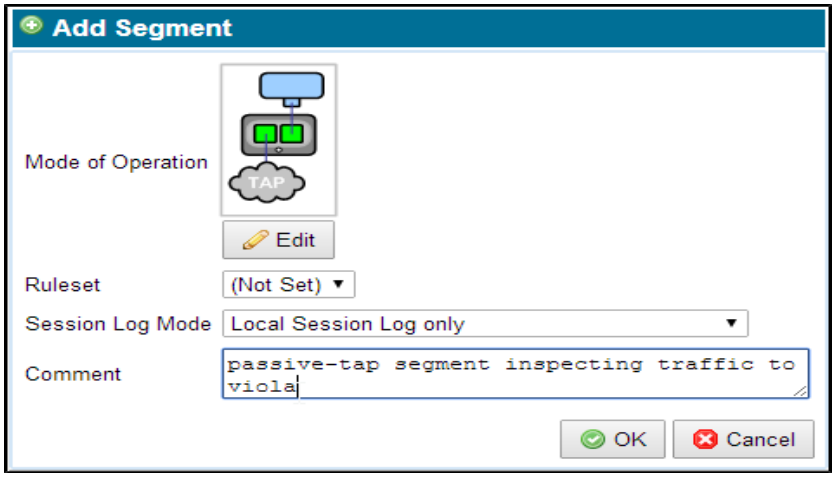


Figure 7.7: Passive-Tap Segment Configuration

Clicking the OK button shown in Figure 7.7 will create the segment, once the **Ruleset** has been selected. At the bottom of the screen, click Apply to complete the process a **Policy Changes** area with buttons to Apply or Cancel the change. and to save the rule to disk.

Once created the segment can be seen in the **Segments** table and can be selected by clicking on it as shown in Figure 7.8. There are three panels below the **Segment** panel in this table, each of which allow different types of actions to be configured for the selected segment. In this example the default values are OK so there is no need for further editing.

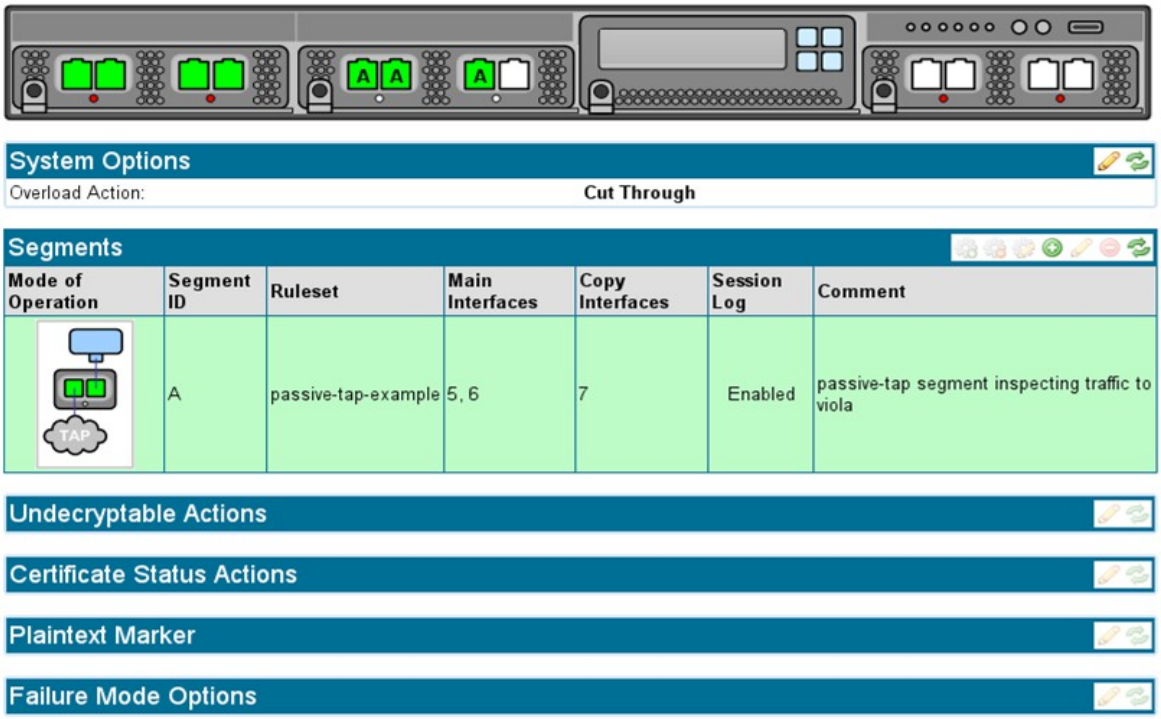


Figure 7.8: Passive-Tap Segment Options and Activation

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Notice that the **Interface** column in the **Segment** shows interface numbers; these are allocated when the segment is activated.

Activation is done by clicking on the Activate button for the segment which is in the tool block at the top right of the segment panel.

During the activation process, a series of screens appear where you select the ports to be used for the segment, and also select any copy ports and the modes that the copy ports will operate in. The initial screen, shown in Figure 7.9, indicates which interfaces on the device are available for use and which are already in use by other segments. In this example no other interfaces are in use.

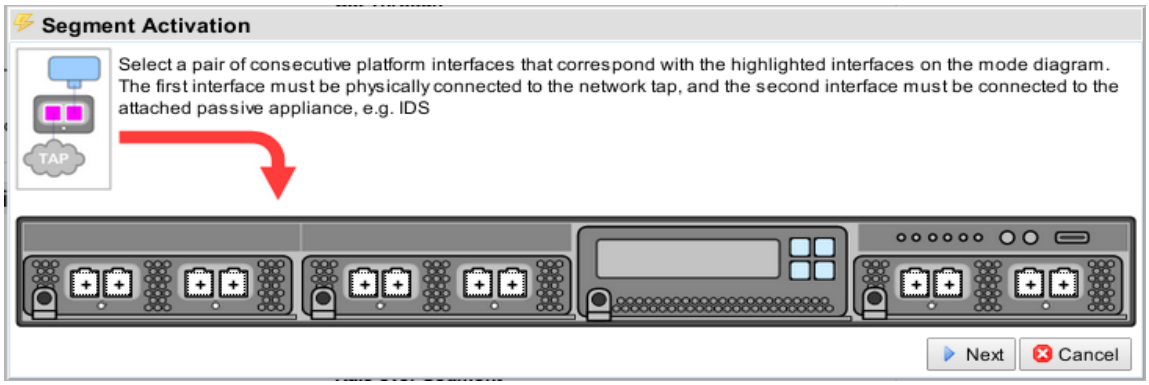


Figure 7.9: Activating a Passive-Tap Segment - Step 1

Figure 7.10 shows that ports 5 and 6 on the device have been selected as the two primary ports for this segment. Clicking on the Next button will move on to the next step in the process.

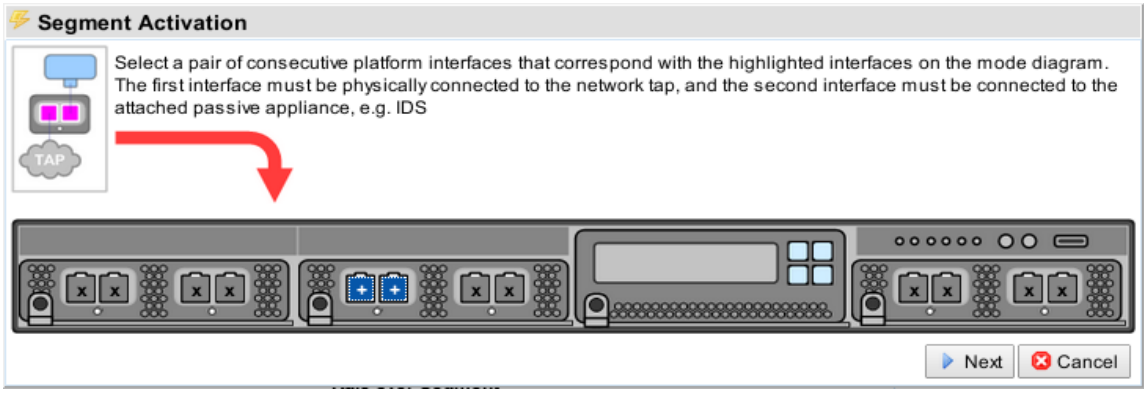


Figure 7.10: Activating a Passive-Tap Segment - Step 2

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 7.11 shows that one or two mirror ports can be configured for this passive tap segment, indicated by the images in the box at top left. One mirror port has been selected in this case. If two mirror ports had been selected then the options allowing selection of per-direction copy or load balancing would be active allowing selection of these capabilities if required. Clicking on the Next button will finish the activation process. The Apply button at the bottom left of the screen will need to be pressed to complete the process.

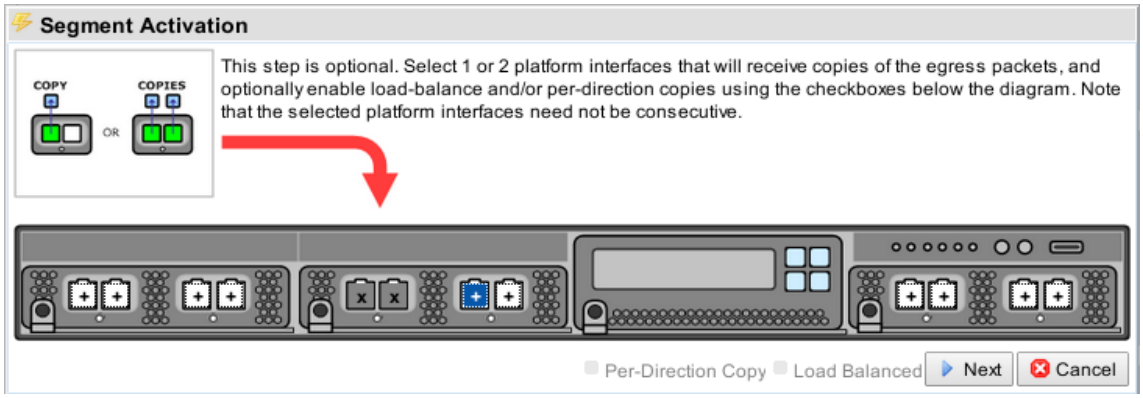


Figure 7.11: Activating a Passive-Tap Segment – Step 3

Once the segment is active the **Segment** screen will show an entry for the new segment, and the graphic at the top of the screen will indicated the ports being used by the segment; see Figure 7.12. In this example, the segment is identified as Segment A, and the ports being used all show the letter A.

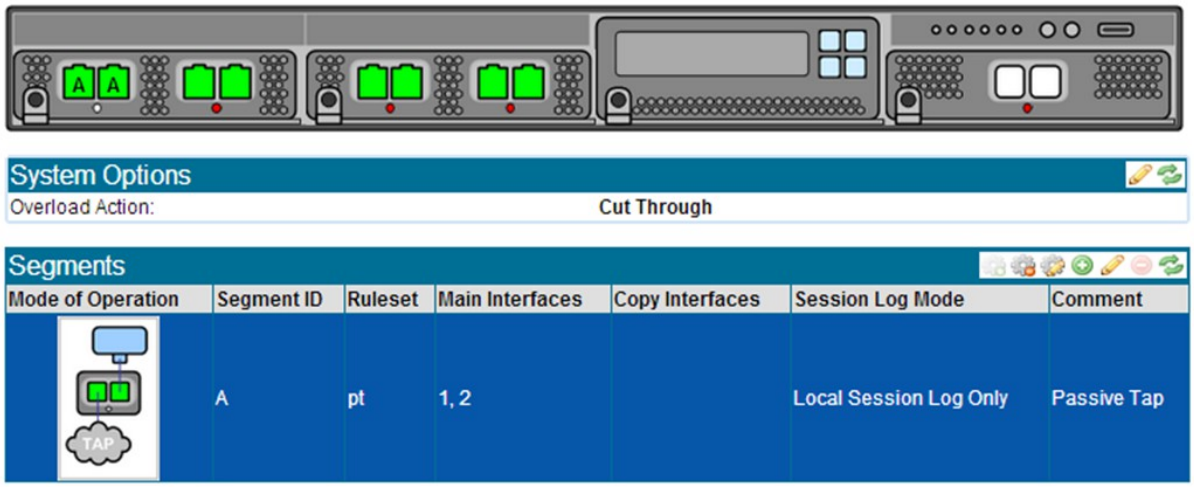


Figure 7.12: Segment with Active Passive-Tap Segment

The green background indicates that this segment is activated. If there is SSL traffic to the server then the SSL session log and SSL statistics screens should show this. See Section 9. for details on the session log and other monitoring tools.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

8. Example Active-Inline Mode Inspection

The following example shows the steps needed to configure the Sourcefire SSL appliance to inspect traffic and to pass the inspected traffic through an Active-Inline security appliance. In this example the Sourcefire SSL appliance is deployed in-line and has an in-line security appliance, such as an IPS, attached. The configuration described below uses four network ports on the SSL2000. The steps involved are:

- Create or load an Internal CA certificate and key into the Sourcefire SSL appliance (Section 6.1)
- Create a ruleset that contains a rule to inspect traffic using certificate resign
- Create a segment for active-inline operation
- Activate the segment to start inspection

Creating a ruleset is a two-step process and is explained in Section 7. In this example the ruleset is called active-inline-example. After creating the ruleset name click OK and the new entry will appear as a row in the Rulesets panel. At the bottom of the screen is a **Policy Changes** area with buttons to Apply or Cancel the change. Click Apply to complete the process and to save the ruleset to disk.

Now click on the active-inline-example row to select it. This will cause the **Ruleset Options** for this ruleset to be displayed (Figure 8.1). Click on the edit tool, , and change the **Trusted Certificates** setting to **All Trusted Certificates**.

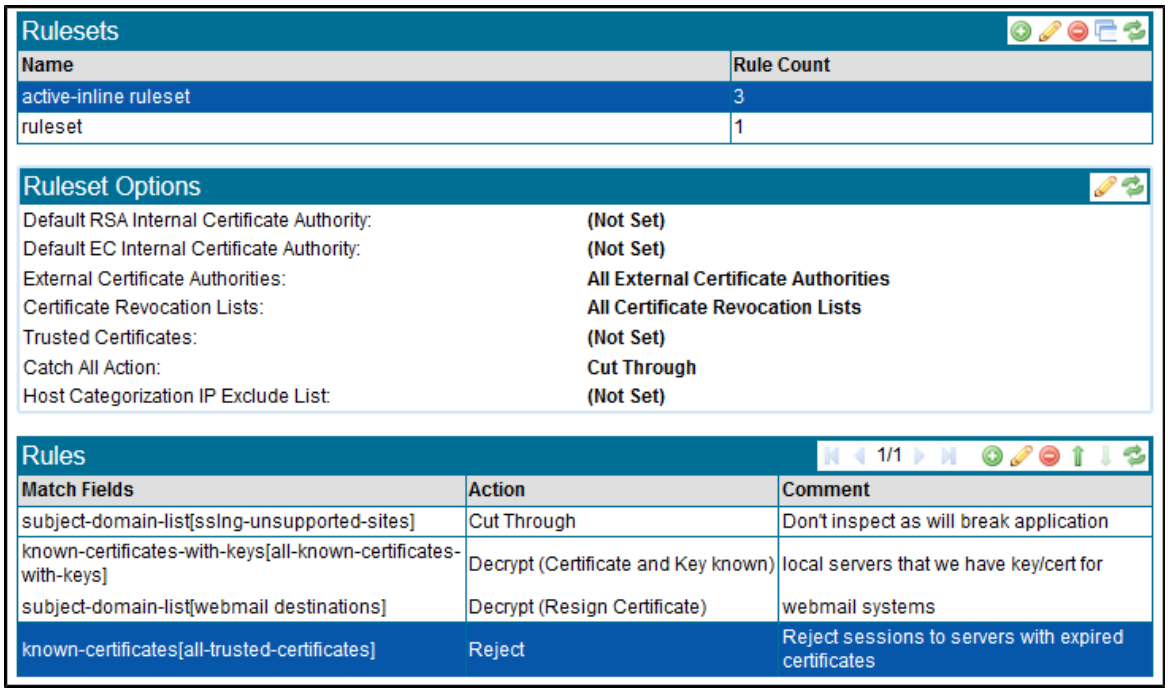


Figure 8.1: Active-Inline Ruleset Options

The **Rules** panel will also appear when the ruleset row is selected. Clicking on the Add button, , will cause the **Insert Rule** form (Figure 8.2) to appear and selecting **Decrypt (Resign Certificate)** on the drop-down menu in this form will allow a rule to be configured. In this example the rule applies to all SSL sessions that pass through the SSL2000. The *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200* provides more details on the options

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

available when creating a rule and how they can be used to create specific rules that only apply to traffic to particular destinations.

Apart from adding a comment to the **Comment** box, no other options are used in this rule so the Save button can be pressed to create the rule. At the bottom of the screen is a **Policy Changes** area with buttons to Apply or Cancel the change. Click Apply to complete the process and to save the rule to disk.

The above rule will inspect all SSL traffic passing through the appliance. By specifying a particular **Subject/Domain Name** or a list that contains multiple **Subject/Domains**, a rule that will only inspect traffic going to particular SSL servers can be created. The Sourcefire SSL appliance extracts CN, Subject Alternative Name (SAN), and Server Name Indication (SNI) information from intercepted flows in order to deduce the SSL server domain name.

When specifying the **Subject/Domain Name** a wild card "*" can be used at the start of the name. For example, a **Subject/Domain Name** value of "*company.com" would match the Common Name (CN) in the server certificates from servers with CNs such as "mail.company.com", "server1.company.com" etc.

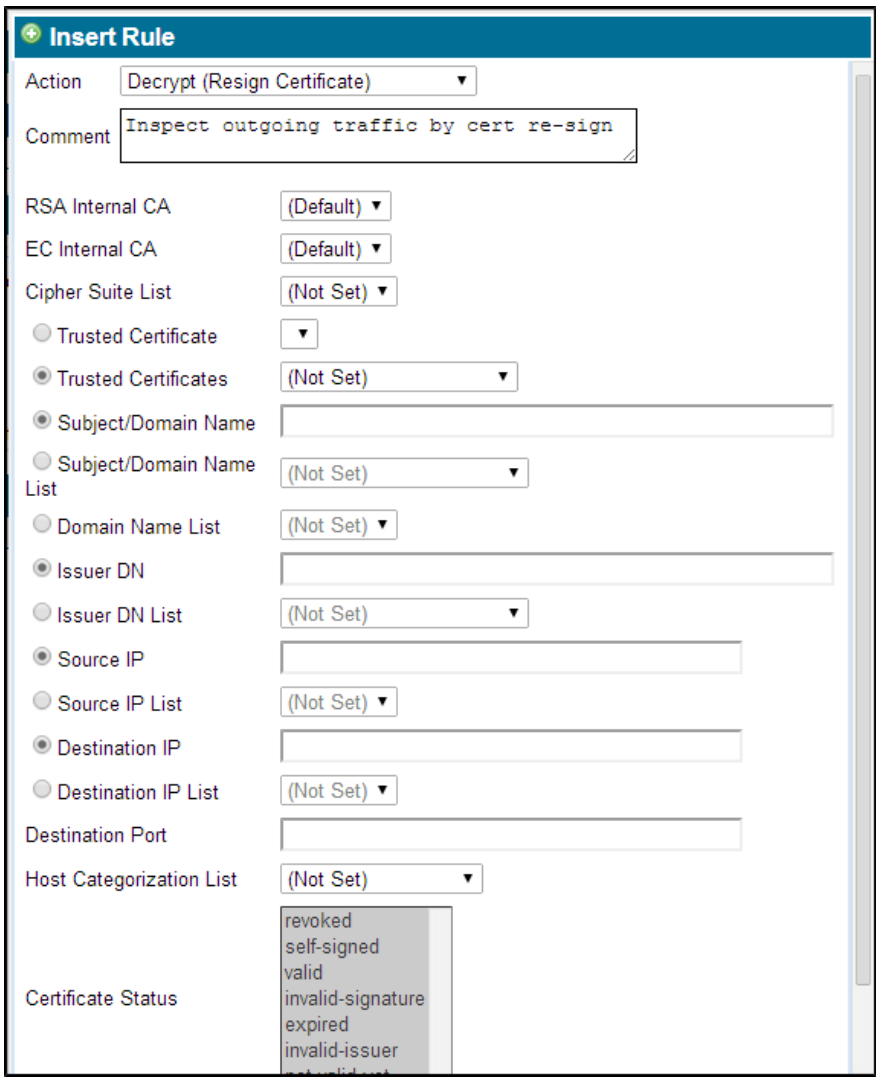


Figure 8.2: Add Rule to Decrypt using Certificate Resign

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The final part of the process is to create a segment, configure it to use the ruleset just created and then to activate it. To create a Segment go to the **Policies > Segments** menu option and you will see the **Segments** panel. Initially there will be no segments configured in the system. To create a new segment click on Add in the **Segments** panel. Figure 8.3 shows the initial form. The Mode of Operation is selected by clicking on the Edit button and then choosing from the **Select Mode of Operation** form the required mode. The **Ruleset** is chosen from the drop-down menu.

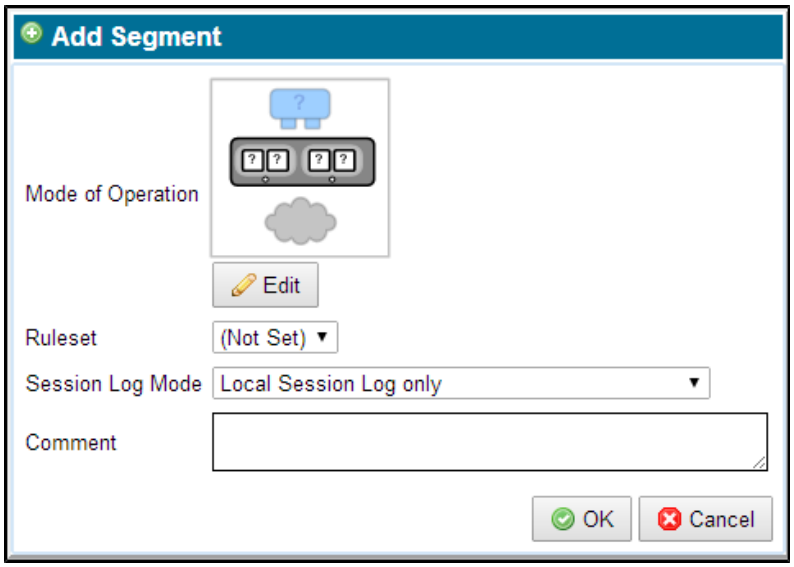


Figure 8.3: Add Segment

Figure 8.4 shows the form used to select the mode of operation for a segment. The **Mode of Operation** area has a scroll bar and displays all the different operating modes as images. The **Main Mode** drop-down menu allows the set of operating modes to be narrowed; by choosing only Active Inline this will reduce the number of options displayed in the **Mode of Operations** area. Clicking on the image for the desired operating mode selects it and clicking Save will set this as the mode of operation for the segment.

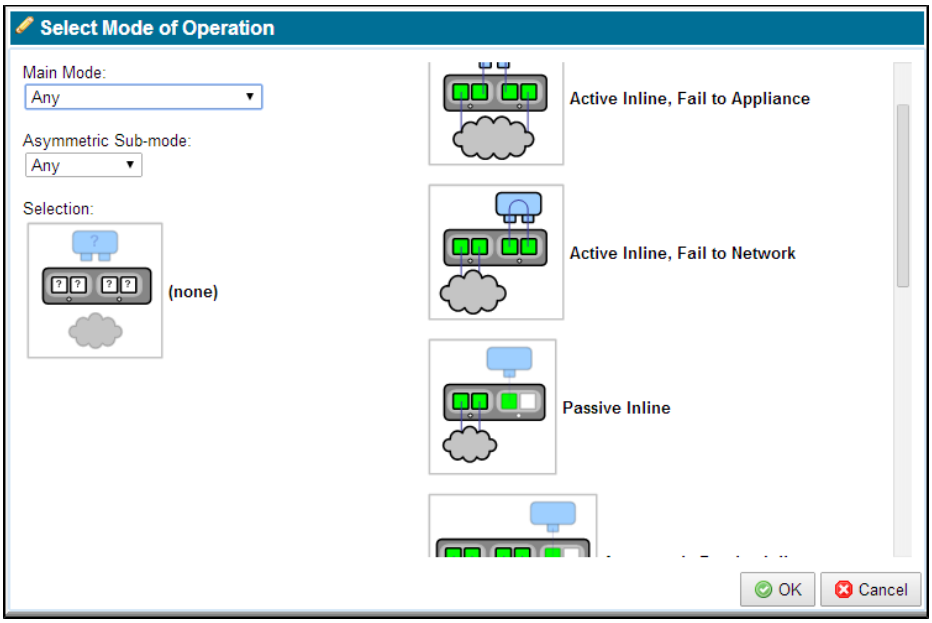


Figure 8.4: Selecting Mode of Operation for a Segment

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 8.5 shows the completed segment details before they are saved. In this example the session log has been enabled and the segment is using the "active-inline-example" ruleset that was created earlier. The graphic in the field indicates that this segment will make use of four ports on the system. The actual port numbers to be used are not known at this point; they are determined when the segment is activated.

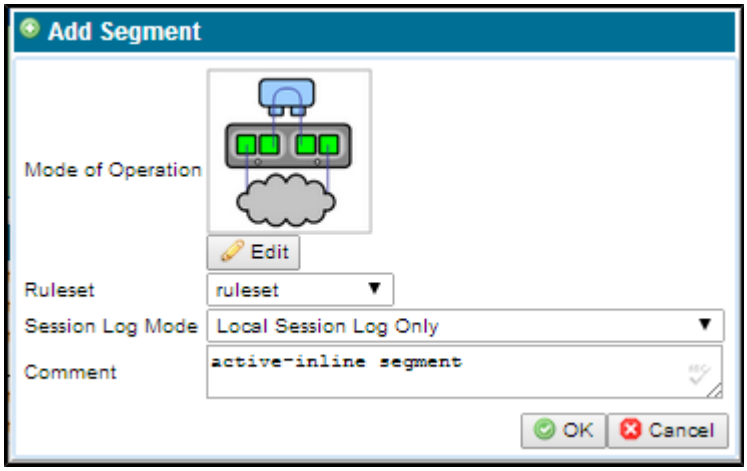


Figure 8.5: Adding an Active-Inline Fail To Appliance Segment

Clicking the OK button shown in Figure 8.5 will create the segment. At the bottom of the screen is a Policy Changes area with buttons to Apply or Cancel the change. Click Apply to complete the process and to save the configuration to disk.

Once created the segment can be seen in the **Segments** table and can be selected by clicking on it. There are three panels below the **Segment** panel in this table, each of which allow different types of actions to be configured for the selected segment. In this example the default values are OK so there is no need for further editing.

Notice that the **Interface** column in the Segment shown in Figure 8.6 does not show interface numbers; these are allocated when the segment is activated. Activation is done by clicking on the Activate button for the segment, which is in the tool block at the top right of the **Segment** panel. During the activation process the user selects the interfaces that are going to be used by the segment and also configures any copy ports and how they should operate.

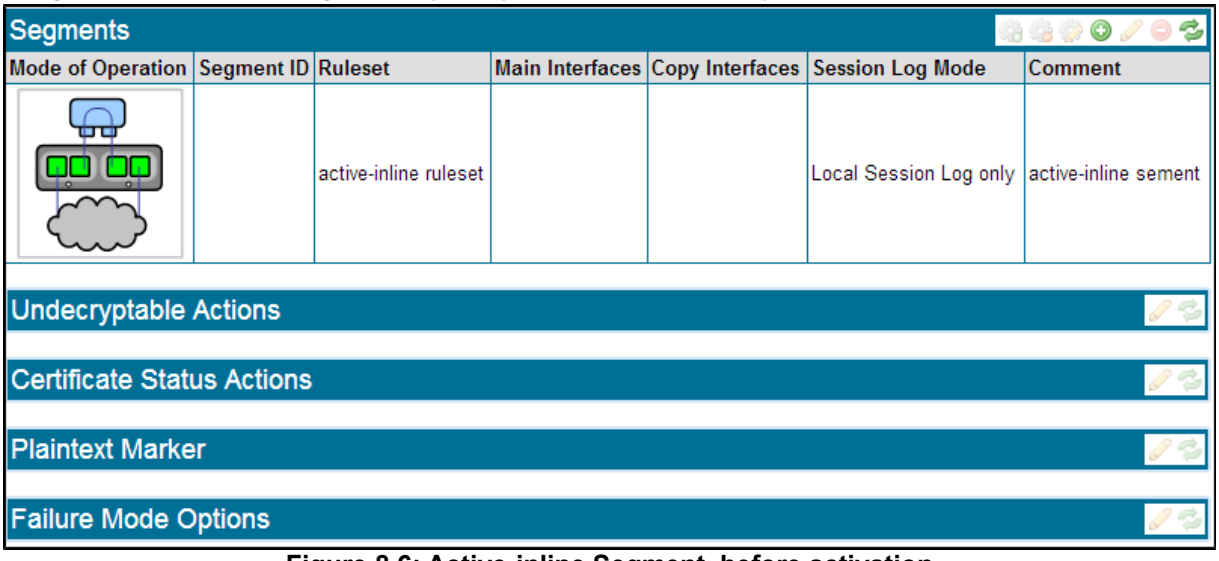


Figure 8.6: Active-inline Segment, before activation

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 8.7 shows he first step in the activation process. The small image on the left indicates the first two ports that need to be allocate highlighted in purple. The text explains that a pair of ports that share a set of fail-to-wire hardware are required. The user selects which pair of interfaces are to be used by clicking on the two interfaces in the diagram of the Sourcefire SSL appliance and then clicking the Next button.

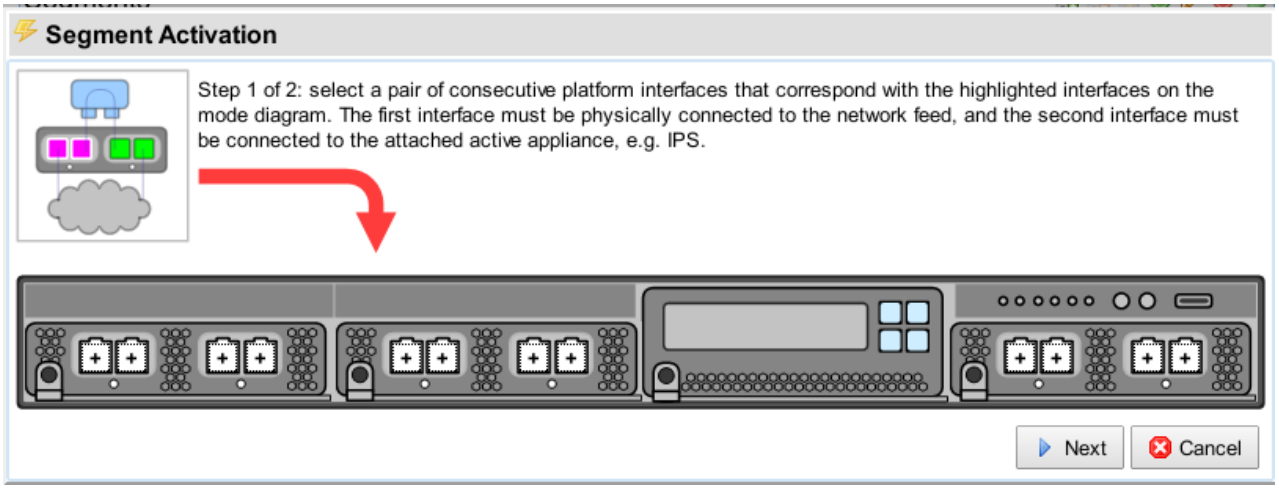
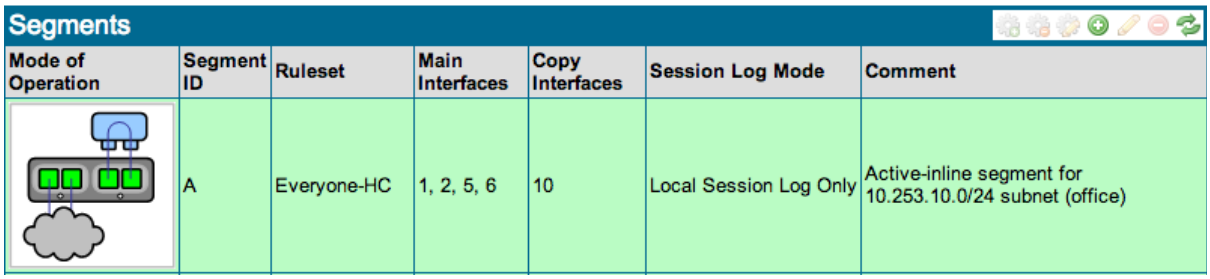


Figure 8.7: Allocating First Pair of Link for an Active-Inline segment

Follow the steps until the segment is active. Figure 8.8 shows the display once the segment is active. Notice that the ports being used by the segment are now identified.



Mode of Operation	Segment ID	Ruleset	Main Interfaces	Copy Interfaces	Session Log Mode	Comment
	A	Everyone-HC	1, 2, 5, 6	10	Local Session Log Only	Active-inline segment for 10.253.10.0/24 subnet (office)

Figure 8.8: Active-Inline Segment Activated

The green background indicates that the segment is activated. If there is SSL traffic to the server then the SSL session log and SSL statistics screens will show this—both these options are under the Monitor menu.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

9. Monitoring the System

The **Monitor** menu, shown in Figure 9.1, contains eight options that provide details on the operation of the system and that allow the collection of diagnostic and debug information. Only the **Dashboard, SSL Session Log** and **SSL Statistics** are described in this document. For more details on monitoring options consult the *Sourcefire SSL Appliance Administration & Deployment Guide for SSL2000 and SSL8200*.

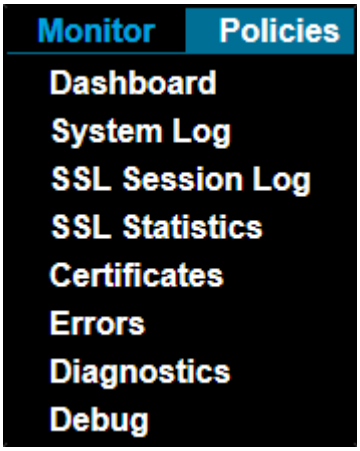


Figure 9.1: Monitor Menu Options

- **Dashboard**: See the overall system status and the status of network links and active segments
- **SSL Session Log**: View details of SSL traffic that is passing through the SSL2000/SSL8200 using the session log
- **SSL Statistics**: View statistics on SSL traffic that is passing through the SSL2000/SSL8200

The session log can be enabled on a per-segment basis. Make sure that it is enabled on the segment you are trying to see details for.

9.1 Dashboard

The dashboard displays several panels containing different types of information, described next.

Figure 9.2: Dashboard Segment Status Panel

Figure 9.2 shows the **Segment Status** panel which displays the status of currently-active segments. The **Segment ID** is a unique identifier that enables this segment to be distinguished from other segments that may be present in the system. The **Interface** numbers identify the physical ports that are being used by this segment. If any of the interfaces being used by the segment are currently down, the interface numbers will show in the **Interfaces Down** column. **Main Mode** indicates the operating mode of the segment, and the **Failures** column will record any failure details.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

The tools available in addition to the Refresh button are:

Manually Unfail tool, which is normally grayed out. It will only be active if the segment is in a failure mode that requires manual intervention to clear the failure.

Manual Fail tool, which is active if a segment is selected. The Manual Fail icon allows a segment to be forced into a failed state.

Figure 9.3 shows the **Network Interfaces** panel. This will have a row for every interface installed in the system, so the maximum number of rows for an SSL2000 is 12 if it is fitted with three 4 x 1Gig Netmods.

Network Interfaces

Port	Type	Link State	RX Packets/Bytes	TX Packets/Bytes	RX Drops
1	1G	1G	18864475/15662763383	19085341/14955569986	0
2	1G	1G	18967611/14946890174	18755544/15616215820	0
3	1G	Down	0/0	0/0	0
4	1G	Down	0/0	0/0	0
5	1G	1G	19955564/14931573650	15165425/15282183930	0
6	1G	1G	15165425/15282183930	19955571/14931583506	0
7	1G	Down	0/0	0/0	0
8	1G	Down	0/0	0/0	0

Figure 9.3: Dashboard Network Interfaces

Each row shows the interface **Type** and the speed it is operating at along with transmit and receive statistics. The tools provided for this panel are the Refresh tool and a Clear Counters tool .

Figure 9.4, **CPU Load %**, shows the current CPU utilization as a percentage of the total capacity of the CPU. The only tool provided for this panel is the refresh button.

CPU Load %

cpu	cpu0	cpu1	cpu2	cpu3	cpu4	cpu5	cpu6	cpu7	cpu8	cpu9	cpu10	cpu11	cpu12	cpu13	cpu14	cpu15
0.2	1.2	0	2.9	0	0	0	0	0	0	0	0	0	0	0	1	0

Figure 9.4: Dashboard CPU Load %

Figure 9.5 shows the **Fan Speed (RPM)** panel which has the current speed values for the various fans in the system. The only tool provided for this panel is the refresh button.

Fan Speed (RPM)

Fan Mod 1 Inlet	Fan Mod 1 Outlet	Fan Mod 2 Inlet	Fan Mod 2 Outlet	Fan Mods 3 to 5	Left Power Supply Fan	Right Power Supply Fan
13276	11860	13876	11592	7237	13157	13157

Figure 9.5: Dashboard Fan Speed (RPM)

Figure 9.6 shows the **Temperatures** panel which includes details of temperatures and thermal margins for components within the system. The only tool provided for this panel is the refresh button.

Temperatures (Degrees °C)

Baseboard Temp	Front Panel Temp	IOH Therm Margin	Mem P1 Thrm Mrgn	Mem P2 Thrm Mrgn	P1 Therm Margin	P2 Therm Margin	NFP0 Temp	Left Power Supply Temp	Right Power Supply Temp
31	25	-43	-35	-48	-53	-60	54	37	41

Thermal margin sensors are reported as negative values which when increased to 0 will cause CPU to throttle down or halt

Figure 9.6: Dashboard Temperatures (Degrees °C)

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Figure 9.7 shows the **Utilization** panel which shows the percentage utilization of system memory and disk space. The Refresh tool is available.

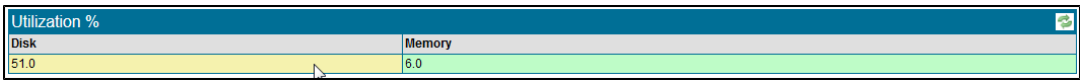


Figure 9.7: Dashboard Utilization %

Figure 9.8 shows the **System Log** panel that contains the most recently generated system log entries, this panel automatically refreshes.

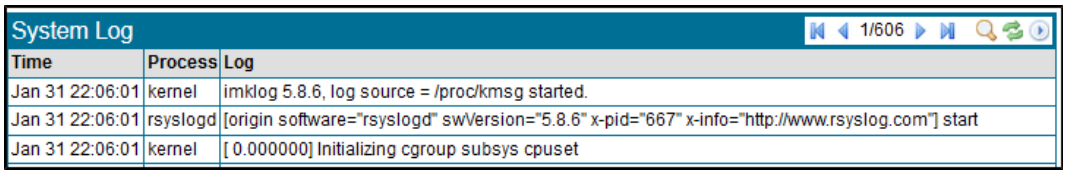


Figure 9.8: Dashboard System Log

9.2 SSL Session Log

The **SSL Session Log** screen (Figure 9.9)contains a single multipage panel enabling all entries in the last 64 pages of the **SSL Session Log** to be viewed. The panel has the standard multipage navigation tools in addition to the Refresh tool, an Export, , tool and two filter tools .

SSL Session Log 1/3414

Start Time	Segment ID	SrcIP:Port	DstIP:Port	Domain Name	Certificate Status	Cipher Suite	Action	Status
Mar 28 10:03:55.142	A	10.253.10.63:49760	10.2.2.154:443	Multiple domains	Invalid Issuer	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:03:24.696	A	10.253.10.62:50293	74.125.239.96:443	SNI: plus.google.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.618	A	10.253.10.62:50292	74.125.239.96:443	SNI: plus.google.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.617	A	10.253.10.62:50291	74.125.239.105:443	SNI: apis.google.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.567	A	10.253.10.62:50290	74.125.239.111:443	SNI: www.gstatic.com		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:24.013	A	10.253.10.62:50289	74.125.239.106:443	lh6.googleusercontent.com	Invalid Issuer	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Decrypt (Resign Certificate)	Success
Mar 28 10:03:23.389	A	10.253.10.103:49877	74.125.239.111:443	ssl.gstatic.com	Invalid Issuer	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:03:20.764	A	10.253.10.63:49759	10.2.2.154:443	Multiple domains	Invalid Issuer	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:03:19.476	A	10.253.10.62:50288	74.125.225.146:443	SNI: www.google.com		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Cut Through	Success
Mar 28 10:02:58.095	A	10.253.10.103:49876	10.253.11.104:443	piranha.pa. example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.093	A	10.253.10.103:49875	10.253.11.104:443	piranha.pa. example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.092	A	10.253.10.103:49874	10.253.11.104:443	piranha.pa. example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.091	A	10.253.10.103:49873	10.253.11.104:443	piranha.pa. example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.088	A	10.253.10.103:49872	10.253.11.104:443	piranha.pa. example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:58.085	A	10.253.10.103:49871	10.253.11.104:443	piranha.pa. example.com	Self Signed	TLS_RSA_WITH_AES_256_CBC_SHA	Decrypt (Resign Certificate)	Success
Mar 28 10:02:54.230	A	10.253.10.103:49870	10.2.2.154:443	Multiple domains	Invalid Issuer	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success

Figure 9.9: SSL Session Log panel

The **Session Log** includes the following details for each SSL session that is recorded in the log:

- Start date and time
- Segment ID for the segment the SSL session occurred on
- IP source and destination address and port number
- Domain details from the server certificate used during the session
- Status of the server certificate
- Cipher Suite that was used for the session
- Action taken by the Sourcefire SSL appliance for this session
- Status for the session

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

Entries in the session log are ordered from most recent to oldest. So, the first row on page 1/64 is the most recent entry and the last row on page 64/64 is the oldest entry.

The filter on errors tool causes the session log to only display entries for flows that were not inspected successfully. The no filter tool causes the session log to revert to showing all entries.

The View Details tool is only active when a row in the **SSL Session Log** panel has been selected. Clicking on the View Details tool will open up a dialog box showing more details about the selected session. Figure 9.10 shows an example of the detail available for a successful session.

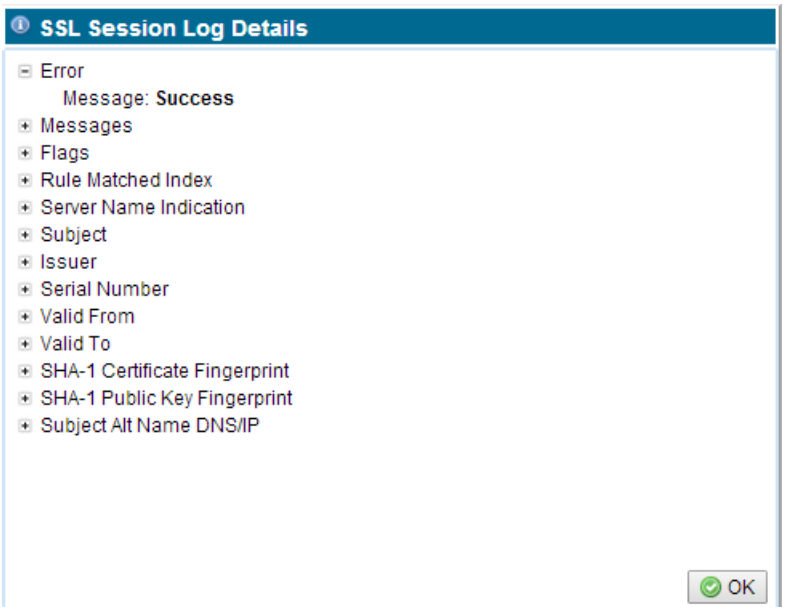
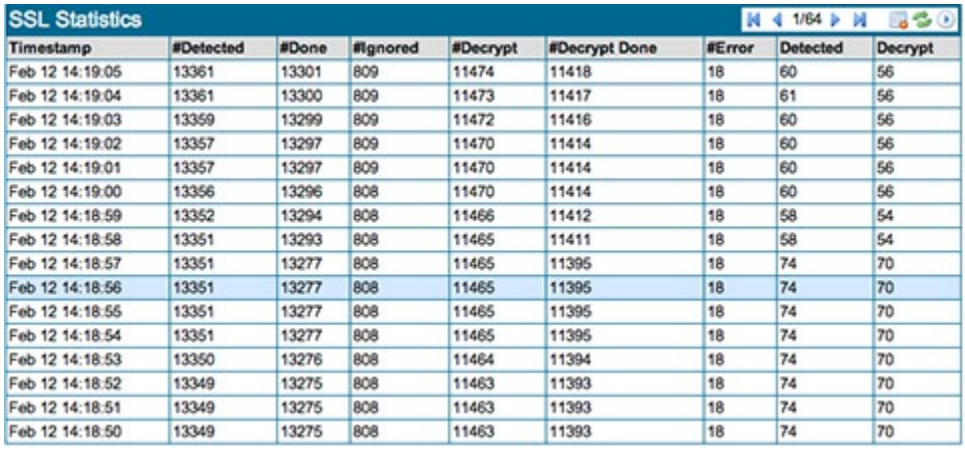


Figure 9.10: SSL Session Detailed Information

9.3 SSL Statistics

The **SSL Session Log** screen contains a single multipage panel enabling all entries in the last 64 pages of the SSL Statistics log to be viewed. The panel has the standard multipage navigation tools, and a Clear Statistics tool.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.



SSL Statistics 1/64

Timestamp	#Detected	#Done	#Ignored	#Decrypt	#Decrypt Done	#Error	Detected	Decrypt
Feb 12 14:19:05	13361	13301	809	11474	11418	18	60	56
Feb 12 14:19:04	13361	13300	809	11473	11417	18	61	56
Feb 12 14:19:03	13359	13299	809	11472	11416	18	60	56
Feb 12 14:19:02	13357	13297	809	11470	11414	18	60	56
Feb 12 14:19:01	13357	13297	809	11470	11414	18	60	56
Feb 12 14:19:00	13356	13296	808	11470	11414	18	60	56
Feb 12 14:18:59	13352	13294	808	11466	11412	18	58	54
Feb 12 14:18:58	13351	13293	808	11465	11411	18	58	54
Feb 12 14:18:57	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:56	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:55	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:54	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:53	13350	13276	808	11464	11394	18	74	70
Feb 12 14:18:52	13349	13275	808	11463	11393	18	74	70
Feb 12 14:18:51	13349	13275	808	11463	11393	18	74	70
Feb 12 14:18:50	13349	13275	808	11463	11393	18	74	70

Figure 9.11: SSL Statistics

Figure 9.11 shows an example where page 1 out of the 64 pages of available statistics information is being displayed. Statistics are collected every second and each row in the table holds the data for a collection interval. Apart from the **Detected** and **Decrypted** columns, all the counts are cumulative. The **Detected** and **Decrypted** columns show the instantaneous number of sessions in each category at the point the data was collected, this is not the total number of sessions that may have been in that category over the one second period. Entries in the **Statistics** panel are ordered from most recent to oldest. So, the first row on page 1/64 is the most recent entry and the last row on page 64/64 is the oldest entry.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.

10. Technical Support

To obtain additional information or to provide feedback, please email support@sourcefire.com or contact the nearest Sourcefire technical support representative.

Visit https://support.sourcefire.com to download the latest documentation and software, access the knowledge base, or log a support ticket.

© 2014 Cisco and/or its affiliates.
All rights reserved. This document is Cisco Public.